Start Here: Where Patient Data Is Protected — and Where It Escapes

The one idea behind every dental AI risk — your practice system is what protects patient information, and the moment data leaves it, that protection is gone.

Start Here: Where Patient Data Is Protected — and Where It Escapes

> You have a dental system for a reason. The biggest AI risk is not the AI — it is taking patient information out of that system.

This guide is the foundation for everything else in the library. It is general educational material for dental practice owners and staff, not legal or clinical advice.

> **Two privacy laws apply in NSW.** As well as the Commonwealth *Privacy Act 1988* and its Australian Privacy Principles (APPs), dental practices in NSW are also bound by the NSW *Health Records and Information Privacy Act 2002* (HRIP Act) and its Health Privacy Principles (HPPs). Read the considerations here against both. General information, not legal advice.

The one idea

Your practice-management system (PMS) is not just where the data lives. It is what *protects* it. It enforces who can see what, records every access in an audit trail, applies retention rules, secures the data, and keeps it inside a boundary you control.

The moment patient information is taken **out** of that system — copied into an email, pasted into ChatGPT, saved to the desktop as a PDF, opened in Word or Canva, synced to a personal cloud drive, dropped into a chat widget, or handed to a marketing tool — **none of that protection comes with it.** The information is now a loose copy, sitting outside the boundary that was built to keep it safe.

That is the core risk. Almost every specific danger in the other guides — overseas processing, the spread of treatment plans, a staff member pasting a name into public AI, an after-hours chatbot storing symptoms — is a *consequence* of patient information leaving the protected system in the first place.

Why it gets worse: extraction starts a cycle

Extraction is not a single event. It is the start of a cycle, because a loose copy tends to make more copies:

- **It gets re-worked, then fed back to AI.** Pulled out, edited in Word to "make it better", pasted into an AI tool to polish, pasted back in. Each round trip is another copy.
- **An AI quietly reads the whole folder.** An "AI assistant" or desktop tool that "reviews your Documents folder" reads every extracted file sitting in Downloads or on the Desktop — including ones you forgot were there.
- **A backup sweeps it up.** That loose file gets caught in an automatic cloud backup — copied again, kept for years, and often stored overseas.

So one extraction becomes many copies, in many places you no longer control, persisting long after the original task is done. That is the engine behind every other risk in this library.

Where it bites: two privacy laws, and the overseas problem

Patient information is health information — the most protected kind. Once it leaves the system, the practice still carries its obligations under **both** the Commonwealth APPs and the NSW HRIP Act, but now without the system's controls helping it meet them. And because so many AI and cloud tools process data **outside Australia**, a loose copy can quietly become a **cross-border disclosure** — which raises **APP 8** considerations (reasonable steps, and the practice generally remaining accountable for what the overseas recipient does). Overseas exposure is, again, a downstream consequence of the data having left the system at all.

The simple rule

You do not need to memorise the law to get this right. The rule is:

> **Keep patient information inside the protected system. The moment a workflow needs to take it out is the moment to stop and check.**

Most "AI projects" that go wrong in a dental practice fail this one test — they quietly move patient data out of the system to make something faster or nicer.

What good looks like

- **One controlled copy.** Keep the authoritative record inside the PMS or an approved system, with its access controls and audit trail intact.
- **Destroy the duplicates, never the record.** Clean up the loose copies that escaped (email attachments, desktop PDFs, Word drafts, personal-drive syncs) — but never delete the authoritative clinical record, which must be kept for a mandatory minimum retention period.

- **Check before anything leaves.** Before patient information is sent to, or processed by, an AI tool, a cloud service, a marketing partner or anyone overseas, treat that as a decision to review — not a default.
- **Public data only in free tools.** Never put patient names, treatment details, images, invoices or identifiable contact details into public AI tools.

Where data escapes — and which guide covers it

Use this guide as your map. Each escape point has its own guide:

- **Staff pasting into public AI** — Can I Paste This Into AI?
- **AI scribes recording consultations** — AI Scribe Consent Checklist
- **Treatment plans leaving the system** — Treatment Plans: Stop The Spread
- **The systems around the PMS** — Dental Privacy Edge Map
- **After-hours booking and chat tools** — Emergency Booking and the AI Boundary
- **AI-assisted owner reporting** — Owner Reporting AI Readiness
- **Website and advertising copy** — Website Advertising AI Review

The honest summary

The dental system was built to protect patient information. AI is not the enemy — but most AI mistakes in a practice come from taking data *out* of that protection to use a tool. Keep it in, check before it leaves, and you have removed the cause of most of the risk before it starts.

This guide is educational material only. It is not legal, privacy or clinical advice. Identifying a risky workflow indicates possible exposure, not a declared breach. Seek qualified advice for your specific circumstances.